

Counting Polynomials with Distinct Zeros in Finite Fields *

Haiyan Zhou^a Li-Ping Wang^b Weiqiong Wang^{c†}

a. School of Mathematics, Nanjing Normal University, Nanjing 210023, China

Email: haiyanxiaodong@gmail.com

b. Institute of Information Engineering, Chinese Academy of Sciences Beijing 100093, China

Email: wangliping@iie.ac.cn

c. School of Science, Chan'an University, Xi'an 710064, China

Email: wqwang@chd.edu.cn

Abstract Let \mathbb{F}_q be a finite field with $q = p^e$ elements, where p is a prime and $e \geq 1$ is an integer. Let $\ell < n$ be two positive integers. Fix a monic polynomial $u(x) = x^n + u_{n-1}x^{n-1} + \cdots + u_{\ell+1}x^{\ell+1} \in \mathbb{F}_q[x]$ of degree n and consider all degree n monic polynomials of the form

$$f(x) = u(x) + v_\ell(x), \quad v_\ell(x) = a_\ell x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x].$$

For integer $0 \leq k \leq \min\{n, q\}$, let $N_k(u(x), \ell)$ denote the total number of $v_\ell(x)$ such that $u(x) + v_\ell(x)$ has exactly k distinct roots in \mathbb{F}_q , i.e.

$$N_k(u(x), \ell) = |\{f(x) = u(x) + v_\ell(x) \mid f(x) \text{ has exactly } k \text{ distinct zeros in } \mathbb{F}_q\}|.$$

In this paper, we obtain explicit combinatorial formulae for $N_k(u(x), \ell)$ when $n - \ell$ is small, namely when $n - \ell = 1, 2, 3$. As an application, we define two kinds of Wenger graphs called jumped Wenger graphs and obtain their explicit spectrum.

Key words Polynomials, Inclusion-Exclusion Principal, Moments Subset-Sum, Distinct Coordinate Sieve, Spectrum of Graphs

1 Introduction

Let \mathbb{F}_q be a finite field with $q = p^e$ elements, where p is a prime and $e \geq 1$ is an integer. Let $\ell < n$ be two positive integers. Fix a monic polynomial $u(x) = x^n + u_{n-1}x^{n-1} + \cdots + u_{\ell+1}x^{\ell+1} \in \mathbb{F}_q[x]$ of degree n and consider all degree n monic polynomials of the form

$$f(x) = u(x) + v_\ell(x), \quad v_\ell(x) = a_\ell x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x].$$

*Research is supported in part by 973 Program (2013CB834203), National Natural Science Foundation of China under Grant No.61202437 and 11471162, in part by Natural Science Basic Research Plan in Shaanxi Province of China under Grant No.2015JM1022 and Natural Science Foundation of the Jiangsu Higher Education Institutes of China under Grant No.13KJB110016.

We are interesting in the number of distinct roots in \mathbb{F}_q of $f(x)$ as the lower degree part $v_\ell(x)$ varies. Since $a^q = a$ for all $a \in \mathbb{F}_q$, we can reduce the polynomial $u(x)$ modulo $x^q - x$. In this way, we can and will assume that $n < q$.

It is clear that $f(x)$ has at most n distinct zeros in \mathbb{F}_q . For integer $0 \leq k \leq n$, let $N_k(u(x), \ell)$ denote the total number of $v_\ell(x)$ such that $u(x) + v_\ell(x)$ has exactly k distinct roots in \mathbb{F}_q , i.e.

$$N_k(u(x), \ell) = |\{f(x) = u(x) + v_\ell(x) \mid f(x) \text{ has exactly } k \text{ distinct zeros in } \mathbb{F}_q\}|.$$

Understanding $N_k(u(x), \ell)$ is an important number theoretical problem with a wide range of applications. For example, in coding theory, $v_\ell(x)$ represents a code word in the $[q, \ell + 1]_q$ Reed-Solomon codes and $u(x)$ represents a received word. The number $N_k(u(x), \ell)$ is then the number of code words whose distance to the received word $u(x)$ is precisely $q - k$. Determining the largest k such that $N_k(u(x), \ell) > 0$ is equivalent to computing the error distance from the received word $u(x)$ to the code, which is the most important problem in decoding Reed-Solomon codes, see [11][14][23] for various partial results. In the special case $k = n$ (the polynomial $f(x)$ splits as a product of n distinct linear factors), the possible large size for $N_n(u(x), \ell)$ is the key to prove several complexity results in decoding primitive Reed-Solomon codes [3] and in approximating the minimum distance of linear codes [4]. For another example, in graph theory, $N_k(u(x), \ell)$ represents the multiplicity of certain eigenvalue in an important class of algebraic graphs extending the classical Wenger graph, see [2]. Deciding this multiplicity is a difficult problem in general.

Mathematically, the number $N_k(u(x), \ell)$ becomes increasingly more complicated as $n - \ell$ grows. Thus, we cannot expect an explicit formula for $N_k(u(x), \ell)$ if $n - \ell$ is large. In the simplest case $n - \ell = 1$, A. Knopfmacher and J. Knopfmacher derived an explicit combinatorial formula for $N_k(u(x), \ell)$ in [7]. Using this formula, S.M. Cioabă, F. Lazebnik and W. Li obtained the explicit spectrum of Wenger graphs in [5]. In this paper, we obtain explicit combinatorial formulae for $N_k(u(x), \ell)$ when $n - \ell$ is small, namely when $n - \ell = 1, 2, 3$. In the case $n - \ell = 1$, we give a simple proof as a simple application of the inclusion-exclusion principal. In the case $n - \ell = 2$, we use the inclusion-exclusion principle together with the subset sum result in [12]. In the case $n - \ell = 3$, it is more complicated. When $k = n$, this is an extension of the subset sum problem up to 2 moments (called Moments Subset-Sum with parameter 2). For a fixed $d \geq 1$, the Moments Subset-Sum with parameter d is formally defined as follows, see [6]:

Moments Subset-Sum(MSS(d)): Given a set $A = \{a_1, \dots, a_n\}$, $a_i \in \mathbb{F}_q$, integer t , and $m_1, \dots, m_d \in \mathbb{F}_q$, decide if there exists a subset $S \subseteq A$ of size t , satisfying $\sum_{a \in S} a^i = m_i$ for all $1 \leq i \leq d$.

Note that MSS(1) is the usual subset sum problem and it is well-known for the NP-hardness of subset sum problem. However, it turns out to be much more difficult to prove NP-hardness for MSS(d) for $d \geq 2$. In 2015, V. Gandikota, B. Ghazi and E. Grigorescu proved the NP-hardness for MSS(d) for $d = 2, 3$, see [6]. Surprisingly, when the degree of the extension $\mathbb{F}_q/\mathbb{F}_p$ is even, $A = \mathbb{F}_q$, $t = n$, $m_i = 0$ and $d = 2$, we obtain

an explicit combinatorial formula for the number of S , i.e., Theorem 4.1, employing the more advanced sieving formula from [13] together with results on quadratic equations over finite fields. Finally, we get explicit combinatorial formulae for $N_k(x^n, n-3)$ using the inclusion-exclusion principal together with Theorem 4.1. As an application, we define two kinds of Wenger graphs called jumped Wenger graphs and obtain their explicit spectrum. Note that in the cases $n-\ell = 2, 3$, the smallest k such that $N_k(u(x), \ell) > 0$ is determined in [15] by giving an explicit construction of a solution. Our result gives an exact and explicit formula for $N_k(u(x), \ell)$.

2 The case $n - \ell = 1$

In this simplest case, using the generating function over an additive arithmetical semigroup, A. Knopfmacher and J. Knopfmacher obtained an explicit combinatorial formula for $N_k(u(x), \ell)$ in [7]. Here, we would give the simple proof according to the classical inclusion-exclusion principal. We recall it briefly.

Let S be a finite set of objects and let P_1, P_2, \dots, P_m be m properties referring to the objects in S . Let $I \subseteq \{P_1, \dots, P_m\}$. Define $S_\emptyset = S$ and $S_I = \{x \in S \mid x \text{ satisfies all properties in } I\}$ for $I \neq \emptyset$. For any non-negative integer j , we put $S_j = \{x \in S \mid x \text{ satisfies exactly } j \text{ properties of } \{P_1, \dots, P_m\}\}$. It is well-known that the classical inclusion-exclusion principal implies

$$|S_j| = \sum_{|I|=j} |S_I| - \sum_{|I|=j+1} |S_I| - \dots + (-1)^{n-j} \sum_{|I|=n} |S_I|, \text{ where } j = 0.$$

It is worth mentioning that the above formula doesn't work for $j \geq 1$. For example, let S be the set consisting of all monic polynomials over \mathbb{F}_2 with degree 3, P_1 the property that the monic polynomial in S has a zero 0, and P_2 the property that the monic polynomial in S has a zero 1. Then it is easy to compute $|S_1| = 4$ and $\sum_{|I|=1} |S_I| - \sum_{|I|=2} |S_I| = 6$.

Theorem 2.1.

$$N_k(x^n, n-1) = q^{n-k} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i}.$$

Proof. Let $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n$ and c_1, c_2, \dots, c_k be k distinct roots of $f(x)$ in \mathbb{F}_q . Then there exists a polynomial $g(x) \in \mathbb{F}_q[x]$ such that $f(x) = (x - c_1)(x - c_2) \dots (x - c_k)g(x)$. For a fixed k -subset $J = \{c_1, \dots, c_k\} \subset \mathbb{F}_q$ and a subset $I \subseteq \mathbb{F}_q - J$, we define the set

$$S_I(J) = \{g(x) \in \mathbb{F}_q[x] \mid g(\alpha) = 0 \text{ for all } \alpha \in I\}.$$

For $0 \leq |I| < n - k$, it is obvious to obtain that the cardinality of the set $S_I(J)$ is $q^{n-k-|I|}$. It follows that for $0 \leq i < n - k$,

$$\sum_{I \subseteq \mathbb{F}_q - J, |I|=i} |S_I(J)| = \binom{q-k}{i} q^{n-k-i}.$$

For $|I| > n - k$, it is clear that $|S_I(J)| = 0$. By the inclusion-exclusion principle, we deduce that

$$\begin{aligned} N_k(x^n, n-1) &= \sum_{|J|=k} \sum_{I \subset \mathbb{F}_q - J} (-1)^{|I|} |S_I(J)| \\ &= \sum_{i=0}^{n-k} (-1)^i \sum_{|J|=k} \sum_{I \subset \mathbb{F}_q - J, |I|=i} |S_I(J)| \\ &= q^{n-k} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i} \end{aligned}$$

□

Remark 2.1. If the degree of $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$ is greater than $q - 1$, i.e., $n \geq q$, then by the Euclidean division, there exist $g(x), h(x) \in \mathbb{F}_q[x]$ such that $f(x) = (x^q - x)g(x) + h(x)$, where $g(x)$ is the monic polynomial with degree $n - q$ and the degree of $h(x)$ is less than q or $h(x) = 0$. If $f(x)$ has exactly $k \leq q - 1$ distinct roots in \mathbb{F}_q , then $h(x)$ has also exactly k distinct roots in \mathbb{F}_q . So we obtain

$$N_k(x^n, n-1) = q^{n-q}(q-1) \sum_{r=k}^{q-1} q^{r-k} \binom{q}{k} \sum_{i=0}^{r-k} (-1)^i \binom{q-k}{i} q^{-i}.$$

Since

$$\begin{aligned} &\sum_{r=k}^{q-1} q^{r-k} \sum_{i=0}^{r-k} (-1)^i \binom{q-k}{i} q^{-i} \\ &= 1 + q \sum_{i=0}^1 (-1)^i \binom{q-k}{i} q^{-i} + \dots + q^{q-1-k} \sum_{i=0}^{q-1-k} (-1)^i \binom{q-k}{i} q^{-i} \\ &= \frac{1}{1-q} \sum_{i=0}^{q-k-1} (-1)^i \binom{q-k}{i} (1 - q^{q-k-i}) \\ &= (q-1)^{q-k-1}, \end{aligned}$$

we have

$$N_k(x^n, n-1) = \binom{q}{k} q^{n-q} (q-1)^{q-k}.$$

If $k = q$, then $h(x) = 0$. Then $N_k(x^n, n-1) = q^{n-q}$. Hence for $n \geq q$,

$$N_k(x^n, n-1) = \binom{q}{k} q^{n-q} (q-1)^{q-k}.$$

3 The case $n - \ell = 2$

In the special case that $k = n$, this is the counting version for the n -subset sum problem over \mathbb{F}_q , which is already handled in [12]. We state this result as a lemma and will use it in our proof.

Lemma 3.1. (See [12]) For $b \in \mathbb{F}_q$, let $M(n, b)$ be the number of n -subsets of \mathbb{F}_q whose elements sum to b . If $p \nmid n$, then

$$M(n, b) = \frac{1}{q} \binom{q}{n}.$$

If $p|n$, then

$$M(n, b) = \frac{1}{q} \binom{q}{n} + (-1)^{n+\frac{n}{p}} \frac{v(b)}{q} \binom{q/p}{n/p},$$

where $v(b) = -1$ if $b \neq 0$, and $v(b) = q - 1$ if $b = 0$.

In terms of our earlier notations, we have $M(n, b) = N_n(x^n - bx^{n-1}, n - 2)$.

Theorem 3.1. (i) If $p \nmid n$, then

$$N_k(x^n - bx^{n-1}, n - 2) = q^{n-k-1} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i}.$$

(ii) If $p | n$, then

$$\begin{aligned} N_k(x^n - bx^{n-1}, n - 2) = & q^{n-k-1} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i} \\ & + (-1)^{\frac{n}{p}+n} \frac{v(b)}{q} \binom{n}{k} \binom{q/p}{n/p}. \end{aligned}$$

Proof. Let c_1, c_2, \dots, c_k be k distinct roots of $f(x)$ in \mathbb{F}_q . Then there exists a polynomial

$$g(x) = x^{n-k} + d_1 x^{n-k-1} + \dots + d_{n-k-1} x + d_{n-k} \in \mathbb{F}_q[x]$$

such that

$$\begin{aligned} f(x) &= x^n - bx^{n-1} + a_2 x^{n-2} + \dots + a_n \\ &= (x - c_1)(x - c_2) \dots (x - c_k) g(x) \\ &= (x^k + b_1 x^{k-1} + \dots + b_{k-1} x + b_k)(x^{n-k} + d_1 x^{n-k-1} + \dots + d_{n-k-1} x + d_{n-k}). \end{aligned}$$

Comparing the coefficients, we have

$$\left\{ \begin{array}{lll} b_1 + d_1 & = & -b \\ b_2 + b_1 d_1 + d_2 & = & a_2 \\ b_3 + b_2 d_1 + b_1 d_2 + d_3 & = & a_3 \\ \dots & \dots & \dots \\ b_k d_{n-k} & = & a_n \end{array} \right.$$

For fixed b and fixed k -subset $J = \{c_1, \dots, c_k\} \subset \mathbb{F}_q$, the coefficient $d_1 = -(b + c_1 + c_2 + \dots + c_k)$ is then fixed. The other coefficients $\{d_2, \dots, d_{n-k}\}$ of the polynomial $g(x)$ are free since $\{a_2, \dots, a_n\}$ are free.

For a subset $I \subseteq \mathbb{F}_q - J$, define the set

$$S_I(J) = \left\{ g(x) = x^{n-k} + d_1 x^{n-k-1} + \cdots + d_{n-k} \in \mathbb{F}_q[x] \mid d_1 = b - (c_1 + c_2 + \cdots + c_k), \right. \\ \left. g(\alpha) = 0 \text{ for all } \alpha \in I \right\}.$$

For $0 \leq |I| < n - k$, the above argument shows that the cardinality of the set $S_I(J)$ is $q^{n-k-1-|I|}$. It follows that for $0 \leq i < n - k$,

$$\sum_{I \subseteq \mathbb{F}_q - J, |I|=i} |S_I(J)| = \binom{q-k}{i} q^{n-k-1-i}.$$

When $i = n - k$, $f(x)$ is forced to have n distinct roots in \mathbb{F}_q with sum equal to b . Then by Lemma 3.1, we deduce

$$\sum_{|J|=k} \sum_{I \subseteq \mathbb{F}_q - J, |I|=n-k} |S_I(J)| = \begin{cases} \binom{n}{k}^{\frac{1}{q}} \binom{q}{n}, & p \nmid n, \\ \binom{n}{k} \left[\frac{1}{q} \binom{q}{n} + (-1)^{n+\frac{n}{p}} \frac{v(b)}{q} \binom{q/p}{n/p} \right], & p \mid n, \end{cases}$$

For $|I| > n - k$, it is clear that $|S_I(J)| = 0$. By the inclusion-exclusion principle, we deduce that

$$N_k(x^n - bx^{n-1}, n-2) = \sum_{|J|=k} \sum_{I \subseteq \mathbb{F}_q - J} (-1)^{|I|} |S_I(J)| = \sum_{i=0}^{n-k} (-1)^i \sum_{|J|=k} \sum_{I \subseteq \mathbb{F}_q - J, |I|=i} |S_I(J)|.$$

Hence,

$$N_k(x^n - bx^{n-1}, n-2) = \begin{cases} \binom{q}{k} \sum_{i=0}^{n-k-1} (-1)^i \binom{q-k}{i} q^{n-k-1-i} + \\ (-1)^{n-k} \binom{n}{k}^{\frac{1}{q}} \binom{q}{n}, & p \nmid n, \\ \binom{q}{k} \sum_{i=0}^{n-k-1} (-1)^i \binom{q-k}{i} q^{n-k-1-i} + \\ (-1)^{n-k} \binom{n}{k} \left[\frac{1}{q} \binom{q}{n} + (-1)^{n+\frac{n}{p}} \frac{v(b)}{q} \binom{q/p}{n/p} \right], & p \mid n. \end{cases}$$

This Theorem is proved from the fact $\binom{q}{k} \binom{q-k}{n-k} = \binom{n}{k} \binom{q}{n}$. □

Remark 3.1. For $n \geq q$, we can deduce the formula of $N_k(x^n - bx^{n-1}, n-2)$.

1) If $n > q$, then $n-1 > q-1$. Similar arguments to those used in the Remark 2.1 show that

$$N_k(x^n - bx^{n-1}, n-2) = q^{n-q-1} \binom{q}{k} (q-1)^{q-k}.$$

2) If $n = q$, then $f(x) = x^q - x - bx^{q-1} + a_2x^{q-2} + \cdots + a_{q-2}x^2 + (a_{q-1} + 1)x + a_q$.
It is easy to get the following conclusions:

When $b \neq 0$,

$$N_k(x^q - bx^{q-1}, q-2) = \begin{cases} 0 & k = q, \\ \frac{1}{q} \binom{q}{k} ((q-1)^{q-k} - (-1)^{q-k}) & k \leq q-1. \end{cases}$$

When $b = 0$,

$$N_k(x^q - bx^{q-1}, q-2) = \begin{cases} 1 & k = q, \\ 0 & k = q-1, \\ \frac{q-1}{q} \binom{q}{k} ((q-1)^{q-k-1} + (-1)^{q-k}) & k \leq q-2. \end{cases}$$

4 The case $n - \ell = 3$

In this section, we always assume that q is an odd number. Let \mathbb{F}_q^n be the Cartesian product of n copies of \mathbb{F}_q . For convenience, we firstly state some results on the number of common solutions in \mathbb{F}_q^n of the equations

$$\begin{cases} a_1x_1^2 + \cdots + a_nx_n^2 &= a_0, \\ b_1x_1 + \cdots + b_nx_n &= b_0, \end{cases} \quad (4.1)$$

where $a_0, b_0, b_1, \dots, b_n \in \mathbb{F}_q$, $a_1, \dots, a_n \in \mathbb{F}_q^*$, $b_i \neq 0$ for at least one i , $1 \leq i \leq n$, see Exercises 6.31-6.34 in [16].

Lemma 4.1. Denote by $N(n, a_0, b_0)$ the number of common solutions in \mathbb{F}_q^n of the equations (4.1). Put $a = a_1a_2 \cdots a_n$, $b = b_1^2a_1^{-1} + \cdots + b_n^2a_n^{-1}$, $c = b_0^2 - a_0b$. Then

i) For $b \neq 0$, $c = 0$,

$$N(n, a_0, b_0) = \begin{cases} q^{n-2} & \text{if } n \text{ even,} \\ q^{n-2} + q^{(n-3)/2}(q-1)\chi((-1)^{(n-1)/2}ab) & \text{if } n \text{ odd,} \end{cases}$$

where χ is the quadratic character of \mathbb{F}_q .

ii) For $b \neq 0$, $c \neq 0$,

$$N(n, a_0, b_0) = \begin{cases} q^{n-2} + q^{(n-2)/2}\chi((-1)^{n/2}ac) & \text{if } n \text{ even,} \\ q^{n-2} - q^{(n-3)/2}\chi((-1)^{(n-1)/2}ab) & \text{if } n \text{ odd.} \end{cases}$$

iii) For $b = c = 0$,

$$N(n, a_0, b_0) = \begin{cases} q^{n-2} + v(a_0)q^{(n-2)/2}\chi((-1)^{n/2}a) & \text{if } n \text{ even,} \\ q^{n-2} + q^{(n-1)/2}\chi((-1)^{(n-1)/2}a_0a) & \text{if } n \text{ odd,} \end{cases}$$

where v is as in Lemma 3.1.

iv) For $b = 0$, $c \neq 0$, $N(n, a_0, b_0) = q^{n-2}$.

Now, we begin to recall a sieve for distinct coordinate counting, see [13]. Let X be a subset of \mathbb{F}_q^n . Motivated by diverse applications in coding theory and graph theory, it is very interesting to count the number of elements in the set

$$\overline{X} = \{(x_1, \dots, x_n) \in X \mid x_i \neq x_j, \forall i \neq j\}.$$

In [13], J. Li and D. Wan discovered the new sieving formula about $|\overline{X}|$. Let S_n be the symmetric group on $\{1, 2, \dots, n\}$. For a given permutation $\tau = (i_1 i_2 \dots i_{t_1}) \dots (l_1 l_2 \dots l_{t_s})$ with $t_i \geq 1, 1 \leq i \leq s$, define

$$X_\tau = \{(x_1, \dots, x_n) \in X \mid x_{i_1} = \dots = x_{i_{t_1}}, x_{l_1} = \dots = x_{l_{t_s}}\}.$$

Now the symmetric group S_n acts on \mathbb{F}_q^n by permuting coordinates. That is, for given $\tau \in S_n$ and $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, we have

$$\tau \circ x = (x_{\tau(1)}, \dots, x_{\tau(n)}) \in X.$$

X is called symmetric if any $x \in X$ and any $\tau \in S_n, \tau \circ x \in X$. Furthermore, If X satisfies the "strongly symmetric" condition, that is, for any τ and σ in S_n , one has $|X_\tau| = |X_\sigma|$ provided $l(\tau)$ and $l(\sigma)$, then we call X a strongly symmetric set. Let C_n be the set of conjugacy classes of S_n . If X is symmetric, then

$$|\overline{X}| = \sum_{\tau \in C_n} (-1)^{n-l(\tau)} C(\tau) |X_\tau|,$$

where $C(\tau)$ is the number of permutations conjugate to τ and $l(\tau)$ is the number of cycles including the trivial cycle.

A permutation $\tau \in S_n$ is said to be of type (c_1, c_2, \dots, c_n) if τ has exactly c_i cycles of length i . We denote by $N(c_1, c_2, \dots, c_n)$ the number of permutations in S_k of type (c_1, c_2, \dots, c_n) and we have (see [19]),

$$N(c_1, c_2, \dots, c_n) = \frac{n!}{1^{c_1} c_1! 2^{c_2} c_2! \dots n^{c_n} c_n!}.$$

Since two permutations are conjugate if and only if they have the same type, we have $C(\tau) = N(c_1, c_2, \dots, c_n)$.

Lemma 4.2. *Put*

$$S_+(n) = \sum_{\substack{i=1 \\ \sum c_i=n, \sum p \nmid i}}^n N(c_1, c_2, \dots, c_n) \prod_{p \mid i} (-q)^{c_i} \prod_{p \nmid i} (-\sqrt{q})^{c_i},$$

$$S_-(n) = \sum_{\substack{i=1 \\ \sum c_i=n, \sum p \mid i}}^n N(c_1, c_2, \dots, c_n) \prod_{p \mid i} (-q)^{c_i} \prod_{p \nmid i} (-\sqrt{q})^{c_i}.$$

Then

$$S_+(n) = \frac{n!}{2}((-1)^n \alpha(n) + \beta(n)),$$

$$S_-(n) = \frac{n!}{2}((-1)^n \alpha(n) - \beta(n)),$$

where

$$\alpha(n) = \sum_{i+pj=n, 0 \leq i \leq \sqrt{q}} \binom{\sqrt{q}}{i} \binom{\frac{q-\sqrt{q}}{p}}{j}$$

and

$$\beta(n) = \sum_{i+pj=n, i \geq 0} (-1)^j \binom{\sqrt{q}-1+i}{\sqrt{q}-1} \binom{\frac{q+\sqrt{q}}{p}}{j}.$$

Proof. Define the generating function

$$C_n(t_1, t_2, \dots, t_n) = \sum_{\sum_{i=1}^n i c_i = n} N(c_1, c_2, \dots, c_n) t_1^{c_1} t_2^{c_2} \dots t_n^{c_n}.$$

Then we get the following exponential generating function

$$\sum_{n \geq 0} C_n(t_1, t_2, \dots, t_n) \frac{u^n}{n!} = e^{ut_1 + u^2 \frac{t_2}{2} + u^3 \frac{t_3}{3} + \dots}.$$

For given generating function $f(x)$, denote by $[x^i]f(x)$ the coefficient of x^i in the formal power series expansion of $f(x)$.

1) If $t_i = -\sqrt{q}$ for $p \nmid i$ and $t_i = -q$ for $p|i$, then we have

$$\begin{aligned} C_n(-\sqrt{q}, \dots, -\sqrt{q}, -q, -\sqrt{q}, \dots, -\sqrt{q}, -q, \dots) \\ &= \left[\frac{u^n}{n!} \right] e^{-\sqrt{q}(u + \frac{u^2}{2} + \frac{u^3}{3} + \dots) + \frac{-q+\sqrt{q}}{p}(u^p + \frac{u^{2p}}{2} + \frac{u^{3p}}{3} + \dots)} \\ &= \left[\frac{u^n}{n!} \right] e^{\sqrt{q} \ln(1-u) + \frac{q-\sqrt{q}}{p} \ln(1-u^p)} \\ &= \left[\frac{u^n}{n!} \right] (1-u)^{\sqrt{q}} (1-u^p)^{\frac{q-\sqrt{q}}{p}} \\ &= \left[\frac{u^n}{n!} \right] \left(\sum_{i \geq 0} (-1)^i \binom{\sqrt{q}}{i} u^i \right) \left(\sum_{j \geq 0} (-1)^j \binom{\frac{q-\sqrt{q}}{p}}{j} u^{pj} \right) \\ &= n! \sum_{i+pj=n, 0 \leq i \leq \sqrt{q}} (-1)^n \binom{\sqrt{q}}{i} \binom{\frac{q-\sqrt{q}}{p}}{j}. \end{aligned}$$

Similarly, if $t_i = \sqrt{q}$ for $p \nmid i$ and $t_i = -q$ for $p|i$, then we have

$$C_n(\sqrt{q}, \dots, \sqrt{q}, -q, \sqrt{q}, \dots) = n! \sum_{i+pj=n, i \geq 0} (-1)^j \binom{\sqrt{q}-1+i}{\sqrt{q}-1} \binom{\frac{q+\sqrt{q}}{p}}{j}.$$

Thus, this lemma is proved from

$$S_+(n) = \frac{C_n(-\sqrt{q}, \dots, -\sqrt{q}, -q, -\sqrt{q}, \dots) + C_n(\sqrt{q}, \dots, \sqrt{q}, -q, \sqrt{q}, \dots)}{2},$$

$$S_-(n) = \frac{C_n(-\sqrt{q}, \dots, -\sqrt{q}, -q, -\sqrt{q}, \dots) - C_n(\sqrt{q}, \dots, \sqrt{q}, -q, \sqrt{q}, \dots)}{2}.$$

□

Lemma 4.3. *Let $q = p^r$ with $p \neq 2$ and χ be the quadratic character of \mathbb{F}_q . Then $\chi|_{F_p}$ is the trivial character of F_p if and only if r is even.*

Proof. Let g be a primitive element of F_p . Then $\chi|_{F_p}$ is the trivial character of F_p if and only if $\chi(g) = 1$, that is, $x^2 - g = 0$ has a root γ in \mathbb{F}_q . Therefore, $F_p(\gamma) \subseteq \mathbb{F}_q$, i.e., r is even. □

Theorem 4.1. *Let $q = p^{2e}$. Denote by $M(n, 0, 0)$ the number of n -subsets of \mathbb{F}_q whose elements are the solutions of the equations*

$$\begin{cases} x_1^2 + \dots + x_n^2 = 0, \\ x_1 + \dots + x_n = 0. \end{cases} \quad (4.2)$$

i) For $p \nmid n$,

$$M(n, 0, 0) = \frac{1}{q^2} \binom{q}{n} + \frac{q-1}{2\sqrt{q^3}}(\alpha(n) - (-1)^n \beta(n)).$$

ii) For $p|n$,

$$M(n, 0, 0) = \frac{1}{q^2} \binom{q}{n} + \frac{q-1}{q^2} \binom{q/p}{n/p} + \frac{q-1}{2q}(\alpha(n) + (-1)^n \beta(n)).$$

Proof. Let X be the set of all solutions of the equations (4.2). Then X is symmetric, so we have

$$n!M(n, 0, 0) = \sum_{\tau \in C_n} (-1)^{n-l(\tau)} C(\tau) |X_\tau|.$$

For a type (c_1, c_2, \dots, c_n) permutation τ , we have $\sum_{i=1}^n ic_i = n$ and $l(\tau) = \sum_{i=1}^n c_i$. Denote by r the number of the cycles of τ such that the length of it is divisible by p , and denote by s the number of the cycles of τ such that the length of it is not divisible by p . Note that $r + s = l(\tau)$ and $\sum_{p \nmid i} ic_i \equiv n \pmod{p}$.

i) Since $p \nmid n$, we have $s \geq 1$. If $s = 1$, then $|X_\tau| = q^{l(\tau)-1}$. If $s \geq 2$, then by i) of Lemma 4.1, we have

$$|X_\tau| = \begin{cases} q^r q^{s-2} & \text{if } s \text{ is even,} \\ q^r (q^{s-2} + q^{(s-3)/2} (q-1) \chi((-1)^{(s-1)/2} \prod_{p \nmid i} i^{c_i} \sum_{p \nmid i} ic_i)) & \text{if } s \text{ is odd,} \end{cases}$$

Since $q = p^{2e}$, by Lemma 4.3 we have

$$|X_\tau| = \begin{cases} q^{l(\tau)-2} & \text{if } s \text{ is even,} \\ q^{l(\tau)-2} + (q-1) q^{-\frac{3}{2}} \prod_{p \nmid i} q^{c_i} \prod_{p \nmid i} \sqrt{q}^{c_i} & \text{if } s \text{ is odd,} \end{cases}$$

Therefore, we have

$$\begin{aligned}
M(n, 0, 0) &= \frac{1}{n!} \sum_{\substack{i \\ ic_i=n, s \geq 2}} (-1)^{n-l(\tau)} C(\tau) q^{l(\tau)-2} + \frac{1}{n!} \sum_{\substack{i \\ ic_i=n, s=1}} (-1)^{n-l(\tau)} C(\tau) q^{l(\tau)-1} \\
&\quad + \frac{1}{n!} (q-1) q^{-\frac{3}{2}} \sum_{\substack{i \\ ic_i=n, s > 2 \text{ is odd}}} (-1)^{n-l(\tau)} C(\tau) \prod_{p|i} q^{c_i} \prod_{p \nmid i} \sqrt{q}^{c_i} \\
&= \frac{1}{n!} \sum_{i=1}^n (-1)^{n-i} c(n, i) q^{i-2} \\
&\quad + \frac{1}{n!} (q-1) q^{-\frac{3}{2}} \sum_{\substack{i \\ ic_i=n, s \text{ is odd}}} (-1)^{n-l(\tau)} C(\tau) \prod_{p|i} q^{c_i} \prod_{p \nmid i} \sqrt{q}^{c_i} \\
&= \frac{1}{q^2} \binom{q}{n} + \frac{1}{n!} (-1)^n (q-1) q^{-\frac{3}{2}} S_-(n) \\
&= \frac{1}{q^2} \binom{q}{n} + \frac{q-1}{2\sqrt{q^3}} (\alpha(n) - (-1)^n \beta(n)).
\end{aligned}$$

ii) Since $p|n$, we have $s \neq 1$. If $s = 0$, then $|X_\tau| = q^{l(\tau)}$. Denote by CP_n the conjugacy classes in C_n whose every cycle length is divisible by p , and denote by $p(n, i)$ the number of permutations in S_n of i cycles with the length of its each cycle divisible by p . If $s > 0$, then by *iii*) of Lemma 4.1 and 4.3 we have

$$\begin{aligned}
M(n, 0, 0) &= \frac{1}{n!} \sum_{\tau \notin CP_n} (-1)^{n-l(\tau)} C(\tau) |X_\tau| + \frac{1}{n!} \sum_{\tau \in CP_n} (-1)^{n-l(\tau)} C(\tau) |X_\tau| \\
&= \frac{1}{n!} \sum_{\tau \notin CP_n} (-1)^{n-l(\tau)} C(\tau) |X_\tau| + \frac{1}{n!} \sum_{i=1}^n (-1)^{n-i} p(n, i) q^i \\
&= \frac{1}{n!} \sum_{i=1}^n (-1)^{n-i} (c(n, i) - p(n, i)) q^{i-2} + \frac{1}{n!} \sum_{i=1}^n (-1)^{n-i} p(n, i) q^i \\
&\quad + \frac{1}{n!} (q-1) q^{-1} \sum_{\substack{s > 0 \\ \text{is even}}} (-1)^{n-l(\tau)} C(\tau) \prod_{p|i} q^{c_i} \prod_{p \nmid i} \sqrt{q}^{c_i} \\
&= \frac{1}{n!} \sum_{i=1}^n (-1)^{n-i} c(n, i) q^{i-2} + \frac{1}{n!} \frac{q-1}{q^2} \sum_{i=1}^n (-1)^{n-i} p(n, i) q^i \\
&\quad + \frac{1}{n!} (q-1) q^{-1} \sum_{\substack{s \\ \text{is even}}} (-1)^{n-l(\tau)} C(\tau) \prod_{p|i} q^{c_i} \prod_{p \nmid i} \sqrt{q}^{c_i}
\end{aligned}$$

Recall that $\sum_{i=1}^n (-1)^{n-i} p(n, i) q^i = (-1)^{n+\frac{n}{p}} n! \binom{q/p}{n/p}$ (See Lemma 3.1 in [13]) and p is an odd prime number. Therefore,

$$\begin{aligned}
M(n, 0, 0) &= \frac{1}{q^2} \binom{q}{n} + \frac{q-1}{q^2} \binom{q/p}{n/p} + \frac{1}{n!} \frac{q-1}{q} S_+(n) \\
&= \frac{1}{q^2} \binom{q}{n} + \frac{q-1}{q^2} \binom{q/p}{n/p} + \frac{q-1}{2q} (\alpha(n) + (-1)^n \beta(n)).
\end{aligned}$$

□

Corollary 4.1. Let $q = p^{2e}$. Denote by $M'(n, 0, 0)$ the number of n -subsets of \mathbb{F}_q whose elements are the common solutions of the equations

$$\begin{cases} \sum_{1 \leq i < j \leq n} x_i x_j = 0, \\ \sum_{1 \leq i \leq n} x_i = 0. \end{cases} \quad (4.3)$$

Then $M'(n, 0, 0) = M(n, 0, 0)$

Proof. This result follows from the fact that the equations (4.3) are equivalent to the equations (4.2). \square

Let X be the set of all solutions of the equations (4.3) in \mathbb{F}_q^n . Put

$$X_1 = \{(x_1, \dots, x_n) \in X \mid x_i \neq x_j, \forall 1 \leq i \neq j \leq n-1\}.$$

Now the symmetric group S_{n-1} acts on \mathbb{F}_q^n by permuting the first $n-1$ coordinates. The similar arguments of the $|\overline{X}|$ show that

$$|X_1| = \sum_{\tau \in C_{n-1}} (-1)^{n-1-l(\tau)} C(\tau) |X_\tau|,$$

where $C(\tau)$ is the number of permutations conjugate to $\tau \in S_{n-1}$ and $l(\tau)$ is the number of cycles including the trivial cycle. Denote by $M_1(n, 0, 0)$ the number of n -subsets $\{x_1, x_2, \dots, x_n \mid x_i \neq x_j, \forall 1 \leq i \neq j \leq n-1\}$ of \mathbb{F}_q whose elements are the common solutions of the equations (4.3). The similar proof of Theorem 4.1 shows the following theorem:

Theorem 4.2. *Let $q = p^{2e}$. Then*

i) For $p \nmid n$,

$$M_1(n, 0, 0) = \frac{1}{q} \binom{q}{n-1} + \frac{q-1}{2q} (\alpha(n-1) + (-1)^{n-1} \beta(n-1)).$$

ii) For $p \mid n$,

$$M_1(n, 0, 0) = \frac{1}{q} \binom{q}{n-1} + \frac{q-1}{2\sqrt{q}} (\alpha(n-1) - (-1)^{n-1} \beta(n-1)),$$

where

$$\alpha(n-1) = \sum_{i+pj=n-1, 0 \leq i \leq \sqrt{q}} \binom{\sqrt{q}}{i} \binom{\frac{q-\sqrt{q}}{p}}{j}$$

and

$$\beta(n-1) = \sum_{i+pj=n-1, i \geq 0} (-1)^j \binom{\sqrt{q}-1+i}{\sqrt{q}-1} \binom{\frac{q+\sqrt{q}}{p}}{j}.$$

Theorem 4.3. Let $q = p^{2e}$ and $k \leq n - 1$.

(i) If $p \nmid n$, then

$$N_k(x^n, n-3) = q^{n-k-2} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i} \\ + (-1)^{n-k-1} \binom{n-1}{k} \frac{q-1}{2q} D(n-1) + (-1)^{n-k} \binom{n}{k} \frac{q-1}{2\sqrt{q^3}} D(n),$$

where $D(n-1) = \alpha(n-1) + (-1)^{n-1}\beta(n-1)$ and $D(n) = \alpha(n) - (-1)^n\beta(n)$.

(ii) If $p|n$, then

$$N_k(x^n, n-3) = q^{n-k-2} \binom{q}{k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i} + (-1)^{n-k} \frac{q-1}{q^2} \binom{n}{k} \binom{q/p}{n/p} \\ + (-1)^{n-k-1} \binom{n-1}{k} \frac{q-1}{2\sqrt{q}} P(n-1) + (-1)^{n-k} \binom{n}{k} \frac{q-1}{2q} P(n),$$

where $P(n-1) = \alpha(n-1) - (-1)^{n-1}\beta(n-1)$ and $P(n) = \alpha(n) + (-1)^n\beta(n)$.

Proof. Note that

$$\binom{n-1}{k} \binom{q}{n-1} = \binom{q}{k} \binom{q-k}{n-k-1} \text{ and } \binom{n}{k} \binom{q}{n} = \binom{q}{k} \binom{q-k}{n-k}.$$

This result follows from the similar proof of Theorem 3.1. \square

Remark 4.1. 1) In the special case $k = n$, $N_k(x^n, n-3) = M(n, 0, 0)$.

2) For $n \geq q$, the formulae of $N_k(x^n, n-3)$ can be obtained from the similar arguments of Remark 2.1.

i) If $n > q + 1$, then $N_k(x^n, n-3) = q^{n-q-2} \binom{q}{k} (q-1)^{q-k}$.

ii) If $n = q + 1$, then

$$N_q(x^n, n-3) = \begin{cases} 1 & k = q, \\ 0 & k = q-1, \\ \frac{q-1}{q} \binom{q}{k} ((q-1)^{q-k-1} + (-1)^{q-k}) & k \leq q-2. \end{cases}$$

ii) If $n = q$, then

$$N_q(x^n, n-3) = \begin{cases} 1 & k = q, \\ 0 & k = q-1, \quad q-2 \\ \frac{q-1}{q} \binom{q}{k} \left(\frac{(q-1)^{q-k-1}}{q} + (-1)^{q-k-1} (q-k) + (-1)^{q-k} \frac{q+1}{q} \right) & k \leq q-3. \end{cases}$$

5 The spectrum of some jumped Wenger graphs

In [22], Wenger introduced a family of p -regular bipartite graphs and then Lazebnik and Ustimenko arrived at a family of bipartite graphs using a construction based on a certain Lie algebra for a prime power q in [8]. Later, Lazebnik and Viglione gave an equivalent representation of these graphs in [10]. Then another useful representation of these graphs was given in [20], on which we concentrate in this section. All graph theory notions can be found in [1].

Let $m \geq 1$ be a positive integer and $g_k(x, y) \in \mathbb{F}_q[x, y]$ for $2 \leq k \leq m+1$. Let $\mathfrak{P} = \mathbb{F}_q^{m+1}$ and $\mathfrak{L} = \mathbb{F}_q^{m+1}$ be two copies of the $(m+1)$ -dimensional vector space over \mathbb{F}_q , which are called the point set and the line set respectively. If $a \in \mathbb{F}_q^{m+1}$, then we write $(a) \in \mathfrak{P}$ and $[a] \in \mathfrak{L}$. Denote $\mathfrak{G} = G_q(g_2, \dots, g_{m+1}) = (V, E)$ by the bipartite graph with vertex set $V = \mathfrak{P} \cup \mathfrak{L}$ and the edge set E is defined as follows: there is an edge from a point $P = (p_1, p_2, \dots, p_{m+1}) \in \mathfrak{P}$ to a line $L = [l_1, l_2, \dots, l_{m+1}] \in \mathfrak{L}$, denoted by $P L$, if the following m equalities hold:

$$\begin{cases} l_2 + p_2 &= g_2(p_1, l_1), \\ l_3 + p_3 &= g_3(p_1, l_1), \\ &\vdots \\ l_{m+1} + p_{m+1} &= g_{m+1}(p_1, l_1). \end{cases} \quad (5.4)$$

If $g_k(x, y) = x^{k-1}y$, $k = 2, \dots, m+1$, then the graph is just the original Wenger graph denoted by $W_m(q)$ in [5]. The spectrum, the diameter and the automorphism group of $W_m(q)$ were studied in [5], [8], [9] and [21]. In [2], a new class of bipartite graphs called linearized Wenger graphs was introduced. These graphs were defined by (5.4) together with $g_k(x, y) = x^{p^{k-2}}$, $k = 2, \dots, m+1$, which denoted by $L_m(q)$. When $m \geq e$, the spectrum of $L_m(q)$ was explicitly determined using results on linearized polynomials over finite fields. The diameter and girth of $L_m(q)$ also were obtained. Furthermore, the spectrum of a general class of graphs, which defined by $g_k(x, y) = f_k(x)y$ and the mapping $\sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q^{m+1}$; $u \rightarrow (1, f_2(u), \dots, f_{m+1}(u))$ is injective, was studied. The eigenvalues of such a graph were determined and their multiplicities were reduced to counting certain polynomials with a given number of roots over \mathbb{F}_q . That is, for all prime power q and positive integer m , the eigenvalues of \mathfrak{G} , counted with multiplicities, are

$$\pm \sqrt{q N_{F_\omega}}, \quad (\omega_1, \omega_2, \dots, \omega_{m+1}) \in \mathbb{F}_q^{m+1},$$

where $F_\omega(u) = \omega_1 + \omega_2 f_2(u) + \dots + \omega_{m+1} f_{m+1}(u)$ and $N_{F_\omega} = |\{u \in \mathbb{F}_q : F_\omega(u) = 0\}|$. For $0 \leq i \leq q$, the multiplicity of $\pm \sqrt{qi}$ is

$$n_i = |\{\omega \in \mathbb{F}_q^{m+1} : N_{F_\omega} = i\}|.$$

In this section, we use our previous results to get the spectrum of a general class of graphs defined by (5.4) together with polynomials $g_k(x, y) = f_k(x)y \in \mathbb{F}_q[x, y]$, where $f_k(x) = x^{k-1}$, $2 \leq k \leq m$, $f_{m+1}(x) = x^{m+1}$ and $f_k(x) = x^{k-1}$, $2 \leq k \leq m$, $f_{m+1}(x) = x^{m+2}$. These graphs are denoted by $JW_m^1(q)$ and $JW_m^2(q)$ respectively.

Theorem 5.1. For all prime power q and $1 \leq m+1 \leq q-1$, the distinct eigenvalues of $JW_m^1(q)$ are

$$\pm q, \pm\sqrt{(m+1)q}, \pm\sqrt{mq}, \dots, \pm\sqrt{2q}, \pm\sqrt{q}, 0.$$

The multiplicity of the eigenvalue $\pm\sqrt{iq}$ is

$$(q-1) \binom{q}{i} \sum_{d=i}^{m-1} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k} + (q-1)N_i(x^{m+2}, m-1), \quad 0 \leq i \leq m-1$$

and

$$(q-1)N_i(x^{m+1}, m-1), \quad i = m, m+1.$$

Proof. Let $(\omega_1, \omega_2, \dots, \omega_{m+1}) \in \mathbb{F}_q^{m+1}$ and $f(X) = \omega_1 + \omega_2 X + \dots + \omega_m X^{m-1} + \omega_{m+1} X^{m+1}$.

In the case of $f = 0$, $|\{u \in \mathbb{F}_q | f(u) = 0\}| = q$. Thus, $JW_m^1(q)$ has $\pm q$ as its eigenvalues.

For any $0 \leq i \leq m-1$, there exists a polynomial f over \mathbb{F}_q of degree at most $m+1 \leq q-1$, which has exactly i distinct roots in \mathbb{F}_q .

For $i = m, m+1$, it is easy to compute $N_1(m+1, i) > 0$ by Theorem 3.1. Then there exists a polynomial of degree $m+1$ which has exactly i distinct roots in \mathbb{F}_q . Thus by Theorem 2.2 in [2], $JW_m^1(q)$ has $\pm\sqrt{iq}$, $0 \leq i \leq m+1$ as its eigenvalues, and by Theorem 2.1 and Theorem 3.1, we obtain that the multiplicity of the eigenvalue $\pm\sqrt{iq}$ is

$$(q-1) \binom{q}{i} \sum_{d=i}^{m-1} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k} + (q-1)N_i(x^{m+1}, m-1), \quad 0 \leq i \leq m-1$$

and

$$(q-1)N_i(x^{m+1}, m-1), \quad i = m, m+1.$$

□

Similarly, we have the following theorem about the spectrum of $JW_m^2(q)$ by Theorem 4.1.

Theorem 5.2. Suppose that p is an odd prime number and $q = p^{2e}$. If $1 \leq m+2 \leq q-1$, then we have

1)

$$\pm q, \pm\sqrt{(m-1)q}, \pm\sqrt{(m-2)q}, \dots, \pm\sqrt{2q}, \pm\sqrt{q}, 0$$

are the distinct eigenvalues of $JW_m^2(q)$. The multiplicity of the eigenvalue $\pm\sqrt{iq}$ is

$$(q-1) \binom{q}{i} \sum_{d=i}^{m-1} \sum_{k=0}^{d-i} (-1)^k \binom{q-i}{k} q^{d-i-k} + (q-1)N_i(x^{m+2}, m-1), \quad 0 \leq i \leq m-1.$$

2) If $m \leq i \leq m+2$, then $\pm\sqrt{iq}$ are the distinct eigenvalues of $JW_m^2(q)$ if and only if $N_i(x^{m+2}, m-1) > 0$. Furthermore, the multiplicity of the eigenvalue $\pm\sqrt{iq}$ is

$$(q-1)N_i(x^{m+2}, m-1).$$

References

- [1] B. Bollobas, Modern Graph Theory, Springer-Verlag New York, Inc., 1998.
- [2] X. Cao, M. Liu, D. Wan, L. Wang, Q. Wang, Linearized Wenger graphs, Discrete Math., 338(2015), 1595-1602.
- [3] Q. Cheng and D. Wan, Complexity of decoding positive-rate Reed-Solomon code, IEEE Tran. Inf. Theory, 56(10) (2010), 5217-5222.
- [4] Q. Cheng and D. Wan, A deterministic reduction for the gap minimum distance problem, IEEE Tran. Inf. Theory, 58(11) (2012), 6935-6941.
- [5] S.M. Cioabă, F. Lazebnik, W. Li, On the spectrum of Wenger graphs, J. Combin. Theory Ser. B, 107(2014), 132-139.
- [6] V. Gandikota, B. Ghazi, E. Grigorescu, On the NP-Hardness of Bounded Distance Decoding of Reed-Solomon Codes, ISIT, IEEE International Symposium , 2015, 2904-2908.
- [7] A. Knopfmacher and J. Knopfmacher, Counting polynomials with a given number of zeros in a finite field, Linear Multilinear A, 26(1990), 287-292.
- [8] F. Lazebnik, V. Ustimenko, New examples of graphs without small cycles and large size, European J. Combin., 14(1993), 445-460.
- [9] F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrary large girth and large size, Discrete Appl. Math., 60(1995), 275-284.
- [10] F. Lazebnik, R. Viglione, An infinite series of regular edge- but not vertex transitive graphs, J. Graph Theory, 41(2002), 249-258.
- [11] M. Keti and D. Wan, Deep holes in Reed-Solomon codes based on Dickson polynomials, Finite Fields Appl., 40 (2016), 110-125.
- [12] J. Li and D. Wan, On the subset sum problem over finite fields, Finite Fields Appl., 14 (4)(2008), 911-929.
- [13] J. Li and D. Wan, A new sieve for distinct coordinate counting, Sci. China Ser. A , 53(2010), 2351-2362.
- [14] Y. Li and D. Wan, On error distance of Reed-Solomon codes, Sci. China Ser. A, 51(11) (2008), 1982-1988.
- [15] Y. Li and G. Zhu, On the error distance of extended Reed-Solomon codes, Adv. Math. Commun., 10(2) (2016), 413-427.
- [16] R. Lidl, H. Niederreiter, Finite Fields. With a foreword by P.M. Cohn, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
- [17] K. Mellinger, D. Mubayi, Construction of bipartite graphs from finite geometries, J. Graph Theory, 49(1)(2005), 1-10.
- [18] J.-Y. Shao, C.-X. He, H.-Y. Shan, The existence of even cycles with specific lengths in Wenger's graph, Acta Math. Appl. Sin. Engl. Ser., 24(2008), 281-288.
- [19] R. P. Stanley , Enumerative Combinatorica, vol. 1, Cambridge: Cambridge University Press, 1997.

- [20] R. Viglione, Properties of some algebraically defined graphs (Ph.D. thesis), University of Delaware, 2002.
- [21] R. Viglione, On the diameter of Wenger graphs, *Acta Appl. Math.*, 104(2008), 173-176.
- [22] R. Wenger, Extremal graphs with no C^4 's, C^6 's or C^{10} 's, *J. Combin. Theory Ser.B*, 52(1)(1991), 113-116.
- [23] G. Zhu and D. Wan, Computing the error distance of Reed-Solomon codes, *Theory and Applications of Models of Computation*, LNCS, 7287 (2012), 214-224.